RECEIVED
CENTRAL FAX CENTER
JUN 2 1 2007

REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-26 are pending in the application. The Examiner additionally stated that claims 1-26 are rejected. By this amendment, claim 16 is cancelled and claims 1, 6, 8, 17, 20, and 22 are amended. Hence, claims 1-15 and 17-26 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §101

The Examiner rejected claims 1-26 under 35 U.S.C. 101 because the claim are directed to non-statutory subject matter.

Regarding claims 1-21, the Examiner noted that although the preamble of the claims recite "apparatus," the body of the claims include only software components such as "a cryptographic instruction," "keygen logic," and "execution logic." The Examiner added that claims 1-21 neither include any computer hardware component(s) nor positively recite that the cited software components are stored on a computer medium that can be read by a machine. As such, the Examiner asserted that claims 1-21 are directed to software per se which is non-functional descriptive material and non-statutory since the claims do not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result to form the basis of statutory subject matter under 35 U.S.C 101.

In reply, Applicant has amended independent claims 1 and 17 to recite "a keygen unit" in place of "keygen logic" and "an execution unit" in place of "execution logic." Applicant respectfully notes that the term "logic" is a well known and often used term in the

electronic arts to that connotes and aggregation of one or more circuits, microcode, or a combination of circuits and microcode. The specification clearly makes this point. In addition, Applicant has elected to amend claim 1 to add that the cryptographic instruction is disposed within an instruction register. Applicant notes that the above noted amendments are made solely in order to expedite the patent application process. Accordingly, it is requested that the rejections of claims 1 and 17 be withdrawn.

Applicant has made similar amendments to claims depending from claims 1 and 17, as required, and asks that the rejections of claims 2-16 and 18-21 be withdrawn as well.

Regarding claims 22-26, the Examiner stated that the method as claimed does not provide a tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

In reply, Applicant has amended claim 22 to recite that the cryptographic instruction is received from memory and that the user-generated key schedule is employed when executing the one of the cryptographic operations to generate a result of the one of the cryptographic operations, thus clarifying that a tangible result is provided as a result of the method steps. Accordingly, it is requested that the rejection of claim 22 be withdrawn and that the rejections of dependent claims 23-26 be withdrawn as well.

Rejections Under 35 U.S.C. §112

The Examiner rejected claims 9, 10, 12, 14, and 15 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner asserted that the claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically:

Regarding claim 9, the Examiner noted that "a first register, wherein contents of said first register comprises: a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks" was not described in the specification.

Regarding claim 10, the Examiner noted that "the plurality of registers comprises: a second register, wherein contents of said second register comprise a second pointer to a

second memory address, said second memory address specifying a second location in said memory" was not described in the specification.

Regarding claim 12, the Examiner noted that "a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data" was not described in the specification.

Regarding claim 14, the Examiner noted that "the plurality of registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location" was not described in the specification.

Regarding claim 15, the Examiner noted that "the plurality, of registers comprises: a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory [for access of a control word for use in accomplishing said one of the cryptographic operations]" was not described in the specification.

Applicant respectfully traverses the rejections and notes that the registers, pointers, and memory locations are indeed described in the specification and drawings. Referring to FIGURE 3, it is noted that the registers are shown within the group of elements 308-312, and their pointer contents are denoted INPTR (claim 9), OUTPTR (claim 10), KEYPTR (claim 12), IVPTR (claim 14), and CWPTR (claim 15). Likewise, their corresponding memory address locations are shown as locations 326, 327, 324, 326, and 323 respectively.

These elements are described in several areas of the drawings and specification as well. One extract from paragraph [0044] recites:

> "Registers 308-312 point to corresponding locations 323-327 in memory 321 that contain data which is required to perform the prescribed cryptographic operation."

Another extract from paragraph [0046] recites:

> "Prior to execution of the XCRYPT instruction 322, however, instructions within the program flow direct the microprocessor 301 to initialize the contents of registers 308-312 so that they point to locations 323-327 in memory 321 that contain a cryptographic control word 323, an initial cryptographic key 324 or a key schedule 324, an initialization vector 325 (if required), input text 326 for the operation, and output text 327."

In view of the above points, Applicant respectfully requests that the rejections of claims 9-10, 12, and 14-15 be withdrawn.

Rejections Under 35 U.S.C. §102(b)

The Examiner rejected claims 1-4, 6, 8, 16-18, 20, and 22-24 under 35 U.S.C. 102(b) as being anticipated by Ehrsam et al., U.S. Patent 4386234 (hereinafter, Ehrsam). Applicant respectfully traverses the Examiner's rejections.

With regard to claim 1, the Examiner asserted that Ehrsam discloses a cryptographic apparatus for performing cryptographic operation comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user generated key schedule be employed for execution of said one of the cryptographic operations (noting that the terminal data security device also provides an arrangement which permits a variety of applications using a predefined private data encryption key) (column 5, lines 63-65);
- keygen logic, operatively coupled to said cryptographic instruction, configured to direct said computing device to load said user-generated key schedule (noting that with a load key direct operation request to the interface adapter the private data encryption key is loaded directly into the working register) (column 5, lines 65-68);

- and execution logic, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations (stating that this allows subsequent encipher/decipher operations to proceed under control of the private data encrypting key) (column 6, lines 1-5).

Applicant respectfully disagrees with the Examiner's characterization of the teachings of Ehrsam vis-à-vis that subject matter which is recited by claim 1. More specifically, Applicant's invention is directed towards incorporation of the ability to perform cryptographic operations in a microprocessor, or like computing device, where a programmer is enabled to insert a cryptographic instruction into a program flow that directs the computing device, among other operations, to perform a cryptographic operation that includes loading a user-generated key schedule. One advantage of such a configuration is that a separate cryptographic processor or cryptographic co-processor is not required, nor are large encryption/decryption routines required to be stored in memory.

A separate cryptographic processor is what is taught be Erhsam. In particular, Ersham depicts, in FIGURE 1, a data security device which is added to control units, terminals, and a host, in order to provide for encryption/decryption functions. He illustrates a data security device within a terminal in FIGURE 2, which includes the crypto device 12 noted by the Examiner. This data security device 11 is distinct from a processor 2 shown therein.

In contrast, claim 1 recites, in combination with other elements and limitations:

- that a cryptographic instruction is received by a microprocessor as part of a instruction flow executing on said microprocessor; and
- a cryptography unit within an execution unit of the microprocessor.

Erhsam does not teach, suggest, nor provide any motivation for one skilled in the art to consider incorporation of a cryptography unit within execution logic of a microprocessor, nor does he suggest, allude to, or hint that a cryptographic instruction may be provided within an instruction flow executing on the microprocessor, where the cryptographic

instruction prescribes a cryptographic operation, and where the cryptographic instruction prescribes that a user-generated key schedule be employed for execution of the cryptographic operation.

Applicant accordingly requests that the rejection of claim 1 be withdrawn.

With respect to claims 3-4, 6, and 8, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Erhsam. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 3-4, 6, and 8.

By this amendment, claim 16 has been cancelled, thereby rendering the Examiner's rejection moot.

As per claims 17 and 22, the Examiner noted that Ehrsam discloses a cryptographic apparatus and method for performing cryptographic operation comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes that a user-generated key schedule be employed when executing said one of the cryptographic operations (noting that the terminal data security device also provides an arrangement which permits a variety of applications using a pre-defined private data encryption key) (column 5, lines 63-65);
- and keygen logic, operatively coupled to said cryptography unit, configured to direct said device to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations (stating that this allows subsequent encipher/decipher operations to proceed under control of the private data encrypting key) (column 6, lines 1-5)

Applicant has amended claims 17 and 22 as well to more clearly recite that these operations are performed by a cryptographic unit within a microprocessor, and that these

operations are directed via a cryptographic instruction which is provided as part of an instruction flow executing on the microprocessor.

Accordingly, it is requested that the rejections of claims 17 and 22 be withdrawn.

With respect to claims 18 and 20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Erhsam. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18 and 20.

With respect to claims 23-24, these claims depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Erhsam. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 23-24.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 5, 19, and 25 under 35 U.S.C. 103(a) as being unpatentable over Ehrsam in view of Fisher et al., CHES 2001, LNCS 2162, pp 77-92, 2001). Applicant respectfully traverses the Examiner's rejections.

Applicant directs the Examiner's attention to arguments and points provided above in traversal of the rejections of claims 1, 17, and 22 wherein it is shown that Erhsam does not teach or suggest a cryptographic unit which is part of an execution unit in a microprocessor, nor does he teach that cryptographic operations can be directed to be executed on the microprocessor through use of a cryptographic instruction provided in an instruction flow executing on the microprocessor.

Accordingly, since claims 5, 19, and 25 add limitations over that subject matter which has been argued above as being allowable, it is requested that the rejections of claims 5, 19, and 25 be withdrawn.

The Examiner rejected claims 9-15 under 35 U.S.C. 103(a) as being unpatentable over Ehrsam in view of Cooney, US Patent 488802. Applicant respectfully traverses the rejections.

Again, Applicant directs the Examiner's attention to arguments and points provided above in traversal of the rejections of claims 1, 17, and 22 wherein it is shown that Erhsam does not teach or suggest a cryptographic unit which is part of an execution unit in a microprocessor, nor does he teach that cryptographic operations can be directed to be executed on the microprocessor through use of a cryptographic instruction provided in an instruction flow executing on the microprocessor.

Accordingly, since claims 9-15 depend from claim 1 and add limitations over that subject matter which has been argued above as being allowable, it is requested that the rejections of claims 9-15 be withdrawn.

RECEIVED
CENTRAL FAX CENTER
JUN 21 2007

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-15 and 17-26 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicant wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

06/21/2007

Date: _____